Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Juniper Networks M7i and J4300 Routers to Support DHCP and a Compressed Real-Time Protocol enabled Point-to-Point Protocol Connection for an Avaya IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe the steps for configuring Juniper Networks M7i and J4300 routers to support an Avaya IP Telephony infrastructure consisting of Avaya Communication Manager and Avaya IP Telephones. A Main site and a Branch site were connected by the two Juniper routers via a compressed Real-Time Protocol (cRTP) enabled Point-to-Point Protocol (PPP) connection. Dynamic Host Configuration Protocol (DHCP) server functionality was supported by the Juniper Networks J4300 router for all Avaya IP Telephones. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

©2006 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe a solution for configuring the Juniper Networks M7i and J4300 routers to support an Avaya IP Telephony infrastructure. A Main site and a Branch site each have an Avaya Communication Manager server. The sites are connected together via a compressed Real-Time Protocol (cRTP) enabled Point-to-Point Protocol (PPP) connection. An H.323 trunk is configured to route calls between the two sites.

It is common to use the G.729 codec for calls across a low speed link to conserve valuable bandwidth. The bandwidth per G.729 call is about 26.4 kbps over a Point-to-Point protocol link. The bandwidth can be further reduced to around 12 kbps with cRTP. The cRTP feature is based on RFC 2508. cRTP compresses the IP/UDP/RTP packet header from 40 bytes to 2 or 4 bytes. For a G.729 call, these headers make up a considerable amount of overhead, relative to the G.729 voice sample payload. As a result, the cRTP feature offers significant VoIP bandwidth savings when using a low bandwidth codec such as G.729, but less percentage saving when using higher bandwidth such as G.711.

Two methods were used in providing the necessary Quality of Service (QoS) for the VoIP traffic. The Juniper routers first use the DiffServ Code-Point (DSCP) information embedded in the layer-3 IP header to prioritize VoIP traffic, and then use bandwidth reservation to guarantee the required bandwidth for VoIP traffic. The combination of traffic prioritization and bandwidth reservation ensure that VoIP traffic passes through the Wide Area Network (WAN) connection successfully in the presence of network congestion.

In addition the Juniper Networks J4300 router has the capability of supporting Dynamic Host Configuration Protocol (DHCP) server functionality necessary to support option 176 which is used by the Avaya IP Telephones. This functionality was implemented in the network configuration to support all of the Avaya IP Telephones.

©2006 Avaya Inc. All Rights Reserved.

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All Avaya IP Telephones with extension range of 2xxxx are registered with Avaya Communication Manager at the Main site and all Avaya IP Telephones with extension range of 3xxxx are registered with Avaya Communication Manager at the Branch Site. An H.323 trunk, configured between the two Avaya Communication Manager servers, routes calls between the two sites. IP addresses for all Avaya IP Telephones are administered by the Juniper Networks J4300 router serving as a DHCP server.

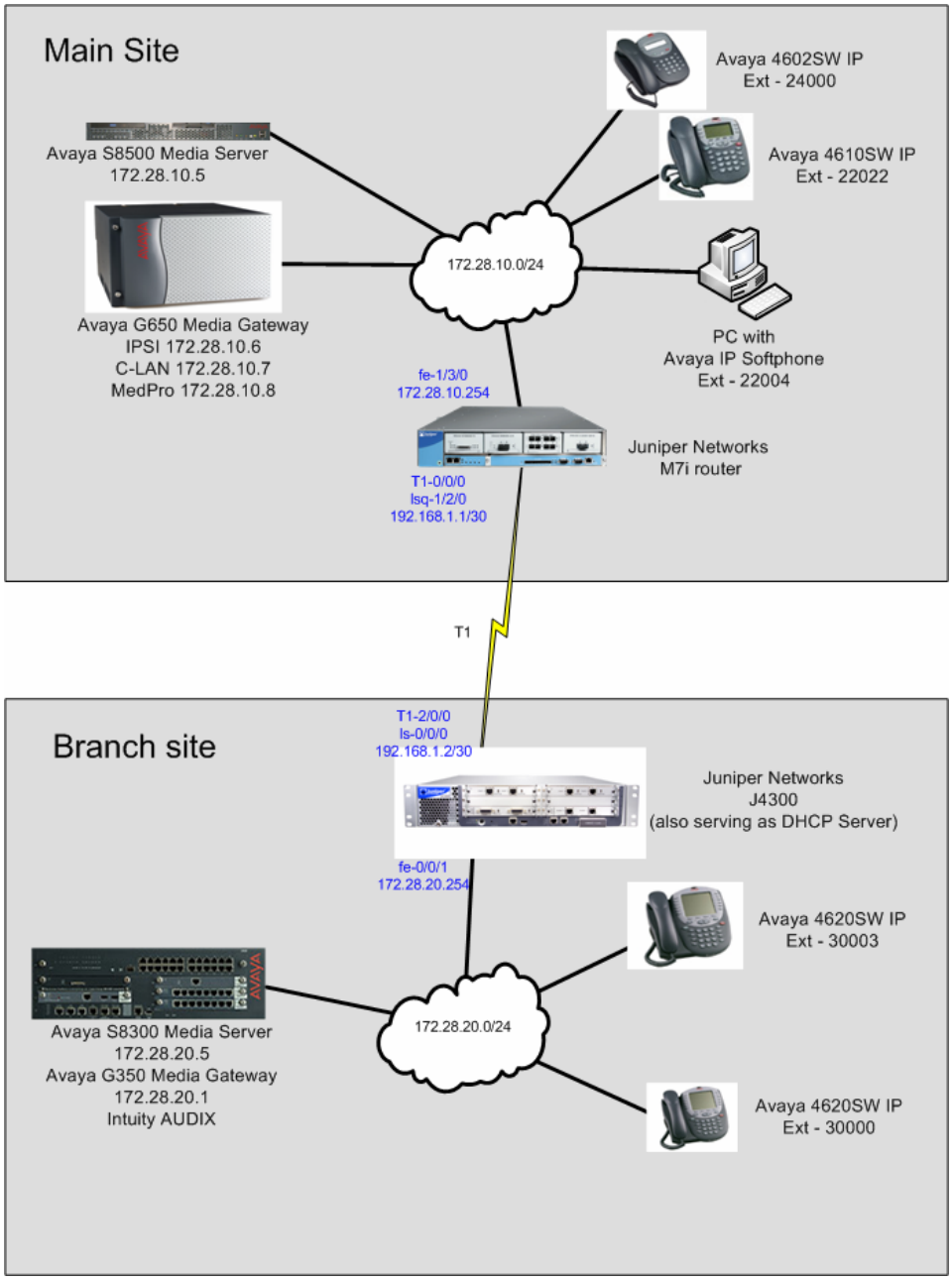

Figure 1: Network Configuration

©2006 Avaya Inc. All Rights Reserved.

3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya S8300 Media Server with G350 Media Gateway	Avaya Communication Manager R3.1 (R03.1-01.0.628.6)
Avaya S8500 Media Server	Avaya Communication Manager R3.1 (R03.1-01.0.628.6)
Avaya G650 Media Gateway	-
TN2312BP IPSI	HW03 FW009
TN799DP C-LAN	HW01 FW015
TN2302AP IP MedPro	HW18 FW108
Avaya 4602SW IP Telephone (H.323)	R2.3 – Application (a02d01b2_3.bin)
Avaya 4610SW IP Telephone (H.323)	R2.3 – Application (a10d01b2_3.bin)
Avaya 4620SW IP Telephone (H.323)	R.2.3 – Application (a20d01b2_3.bin)
Avaya IP Softphone	R5.24.8
Juniper Networks M7i router	JUNOS 7.6R2.6
Juniper Networks J4300 router	JUNOS 7.6R2.6

4. Configure Juniper Networks Routers

This section describes the configuration for Juniper Networks J4300 and M7i routers shown in **Figure 1**.

4.1. Configure the Juniper Networks J4300 router

This section shows the necessary steps in configuring the J4300 router as shown in the network configuration in **Figure 1**. The following steps use the Command Line Interface (CLI) offered by the J4300 router.

Step	Description

1.	Connect to the J4300. Log in using the appropriate Login ID and Password.
	
	`login:`
	`Password:`
	
	A prompt similar to the following will appear after successful log in.
	
	`interop@J4300>`

2.	Enter configuration mode by typing in **edit** at the prompt. `interop@J4300>` *`edit`* `interop@J4300#`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

3.	Configure the **code-point-aliases** and **classifier** for Avaya VoIP traffic.
	
	• The alias helps identify the binary DSCP setting by giving it a name.
	• The sample network uses the name "avaya-rtp" to denote DSCP binary bit 101110 for media traffic. This is equivalent to the decimal **Audio PHB Value** of 46 set in Avaya Communication Manager for RTP Media in Section 5, Step 8.
	• The sample network uses the name "avaya-sig" to denote DSCP binary bit 100010 for signaling traffic. This is equivalent to the decimal **Call Control PHB Value** of 34 set in Avaya Communication Manager for signaling in Section 5, Step 8.
	
	`interop@J4300# edit class-of-service code-point-aliases`
	`interop@J4300# set dscp avaya-rtp 101110`
	`interop@J4300# set dscp avaya-sig 100010`
	`interop@J4300# exit`
	
	• Define a **classifier** called "Avaya-voip".
	• The **classifier** "Avaya-voip" defines the forwarding characteristic of the router based on traffic types.
	• The network is configured to use expedited-forwarding with low loss-priority for "avaya-rtp", and assured-forwarding with low loss-priority for "avaya-sig".
	
	`interop@J4300# edit class-of-service classifiers`
	`interop@J4300# edit dscp Avaya-voip`
	`interop@J4300# set forwarding-class expedited-forwarding loss-priority low code-points avaya-rtp`
	`interop@J4300# set forwarding-class assured-forwarding loss-priority low code-points avaya-sig`
	`interop@J4300# exit`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

4.	Configure the scheduler to specify how much bandwidth to allocate for each type of traffic queue.
	
	• The sample configuration defines **scheduler-maps** "voip" and assigns a name for each of the 4 queues types.
	
	`interop@J4300# edit class-of-service scheduler-maps`
	`interop@J4300# edit voip`
	`interop@J4300# set forwarding-class best-effort scheduler be-sched`
	`interop@J4300# set forwarding-class expedited-forwarding scheduler ef-sched`
	`interop@J4300# set forwarding-class assured-forwarding scheduler af-sched`
	`interop@J4300# set forwarding-class network-control scheduler nc-sched`
	`interop@J4300# exit`
	`interop@J4300# exit`
	
	• Use the scheduler to define the percentage of bandwidth allocation to each traffic queue type.
	
	`interop@J4300# edit class-of-service schedulers`
	`interop@J4300# edit be-sched`
	`interop@J4300# set transmit-rate percent 10`
	`interop@J4300# set buffer-size percent 10`
	`interop@J4300# set priority low`
	`interop@J4300# exit`
	`interop@J4300# edit ef-sched`
	`interop@J4300# set transmit-rate percent 80`
	`interop@J4300# set buffer-size percent 80`
	`interop@J4300# set priority high`
	`interop@J4300# exit`
	`interop@J4300# edit af-sched`
	`interop@J4300# set transmit-rate percent 5`
	`interop@J4300# set buffer-size percent 5`
	`interop@J4300# set priority high`
	`interop@J4300# exit`
	`interop@J4300# edit nc-sched`
	`interop@J4300# set transmit-rate percent 5`
	`interop@J4300# set buffer-size percent 5`
	`interop@J4300# set priority high`
	`interop@J4300# exit`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

5.	Assign the scheduler-map to each interface.
	
	• Configure each interface with **scheduler-map** "voip" using the **classifier** defined above.
	
	`interop@J4300# edit class-of-service interfaces fe-0/0/1`
	`interop@J4300# set unit 0 scheduler-map voip`
	`interop@J4300# set unit 0 classifiers dscp avaya-voip`
	`interop@J4300# exit`
	`interop@J4300# edit class-of-service interfaces ls-0/0/0`
	`interop@J4300# set unit 0 scheduler-map voip`
	`interop@J4300# set unit 0 classifiers dscp avaya-voip`
	`interop@J4300# exit`
	`interop@J4300# edit class-of-service interfaces t1-2/0/0`
	`interop@J4300# set unit 0 scheduler-map voip`
	`interop@J4300# set unit 0 classifiers dscp avaya-voip`
	`interop@J4300# exit`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

6.	Configure the Ethernet and T1 interfaces.
	
	• Configure the Ethernet interface to use the scheduler.
	• Assign an IP address to the interface.
	
	`interop@J4300# edit int fe-0/0/1`
	`interop@J4300# set per-unit-scheduler`
	`interop@J4300# set unit 0 family inet address 172.28.20.254/24`
	`interop@J4300# exit`
	
	• Configure the logical interface for the WAN connection to use the scheduler.
	• Assign an IP address to the interface.
	• Specify the RTP traffic to be compressed. The sample configuration defines RTP traffic with port UDP range 2048 to 3029 to be compressed. This port range needs to match **UDP Port Min** and **UDP Port Max** configured in Avaya Communication Manager in Section 5, Step 8.
	
	`interop@J4300# edit int ls-0/0/0`
	`interop@J4300# set per-unit-scheduler`
	`interop@J4300# set unit 0 compression rtp port min 2048 max 3029`
	`interop@J4300# set unit 0 family inet 192.168.1.2/30`
	`interop@J4300# exit`
	
	• Configure the T1 interface to use the scheduler.
	• Configure the T1 interface timing, encapsulation, and timeslots.
	• Configure the T1 interface to use logical interface ls-0/0/0.0 defined above. An IP address is not necessary because an IP address is already defined for the logical interface.
	
	`interop@J4300# edit int t1-2/0/0`
	`interop@J4300# set per-unit-scheduler`
	`interop@J4300# set clocking external`
	`interop@J4300# set encapsulation ppp`
	`interop@J4300# set t1-options timeslots 1-24`
	`interop@J4300# set unit 0 compression-device ls-0/0/0.0`
	`interop@J4300# exit`

7.	Configure the routing options for the router. The sample configuration uses static routes.
	
	`interop@J4300# edit routing-options static`
	`interop@J4300# route 172.28.10.0/24 next-hop 192.168.1.1`
	`interop@J4300# exit`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

8.	Configure the DHCP Server. The network was configured with 2 pools of IP addresses with each pool serving out IP addresses from x.y.z.128 to x.y.z.191. DHCP option 176 directs Avaya IP Telephones from each site to their respective Avaya Media Server and port.
	
	`interop@J4300# edit system services dhcp pool 172.28.20.0/24`
	`interop@J4300# set address-range low 172.28.20.128 high 172.28.20.191`
	`interop@J4300# set router 172.28.20.254`
	`interop@J4300# set option 176 string MCIPADD=172.28.20.5,MCPORT=1719`
	`interop@J4300# edit system services dhcp pool 172.28.10.0/24`
	`interop@J4300# set address-range low 172.28.10.128 high 172.28.10.191`
	`interop@J4300# set router 172.28.10.254`
	`interop@J4300# set option 176 string MCIPADD=172.28.10.7,MCPORT=1719`
	`interop@J4300# exit`

9.	Save the changes. `interop@J4300# commit`

4.2. Configure the Juniper Networks M7i router

This section shows the necessary steps in configuring the M7i router as shown in **Figure 1**. The following steps use the CLI offered by the router.

Step	Description

1.	Connect to the M7i. Log in using the appropriate Login ID and Password.
	
	`login:`
	`Password:`
	
	A prompt similar to the following will appear after successful log in.
	
	`interop@M7I>`

2.	Enter configuration mode by typing in **edit** at the prompt.
	
	`interop@M7I> edit`
	`interop@M7I#`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

3.	Configure the **code-point-aliases** and **classifier** for Avaya VoIP traffic.
	
	• The alias helps identify the binary DSCP setting by giving it a name.
	• The sample network uses the name "avaya-rtp" to denote DSCP binary bit 101110 for media traffic. This is equivalent to the decimal **Audio PHB Value** of 46 set in Avaya Communication Manager for RTP Media in Section 5, Step 8.
	• The sample network uses the name "avaya-sig" to denote DSCP binary bit 100010 for signaling traffic. This is equivalent to the decimal **Call Control PHB Value** of 34 set in Avaya Communication Manager for signaling in Section 5, Step 8.
	
	`interop@M7I# edit class-of-service code-point-aliases`
	`interop@M7I# set dscp avaya-rtp 101110`
	`interop@M7I# set dscp avaya-sig 100010`
	`interop@M7I# exit`
	
	• Define a **classifier** called "Avaya-voip".
	• The **classifier** "Avaya-voip" defines the forwarding characteristic of the router based on traffic types.
	• The network is configured to use expedited-forwarding with low loss-priority for "avaya-rtp", and assured-forwarding with low loss-priority for "avaya-sig".
	
	`interop@M7I# edit class-of-service classifiers`
	`interop@M7I# edit dscp Avaya-voip`
	`interop@M7I# set forwarding-class expedited-forwarding loss-priority low code-points avaya-rtp`
	`interop@M7I# set forwarding-class assured-forwarding loss-priority low code-points avaya-sig`
	`interop@M7I# exit`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

4.	Configure the scheduler to specify how much bandwidth to allocate for each type of traffic queue.
	
	• The sample configuration defines **scheduler-maps** "voip" and assigns a name for each of the 4 queue types.
	
	`interop@M7I# edit class-of-service scheduler-maps`
	`interop@M7I# edit voip`
	`interop@M7I# set forwarding-class best-effort scheduler be-sched`
	`interop@M7I# set forwarding-class expedited-forwarding scheduler ef-sched`
	`interop@M7I# set forwarding-class assured-forwarding scheduler af-sched`
	`interop@M7I# set forwarding-class network-control scheduler nc-sched`
	`interop@M7I# exit`
	`interop@M7I# exit`
	
	• Use the scheduler to define the percentage of bandwidth allocation to each traffic queue type.
	
	`interop@M7I# edit class-of-service schedulers`
	`interop@M7I# edit be-sched`
	`interop@M7I# set transmit-rate percent 10`
	`interop@M7I# set buffer-size percent 10`
	`interop@M7I# set priority low`
	`interop@M7I# exit`
	`interop@M7I# edit ef-sched`
	`interop@M7I# set transmit-rate percent 80`
	`interop@M7I# set buffer-size percent 80`
	`interop@M7I# set priority high`
	`interop@M7I# exit`
	`interop@M7I# edit af-sched`
	`interop@M7I# set transmit-rate percent 5`
	`interop@M7I# set buffer-size percent 5`
	`interop@M7I# set priority high`
	`interop@M7I# exit`
	`interop@M7I# edit nc-sched`
	`interop@M7I# set transmit-rate percent 5`
	`interop@M7I# set buffer-size percent 5`
	`interop@M7I# set priority high`
	`interop@M7I# exit`

5.	Configure the queue assignment for each traffic type. This is only for the M7i router.
	
	`interop@M7I# edit class-of-service forwarding-classes`
	`interop@M7I# set queue 0 best-effort`
	`interop@M7I# set queue 1 expedited-forwarding`
	`interop@M7I# set queue 2 assured-forwarding`
	`interop@M7I# set queue 3 network-control`
	`interop@M7I# exit`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

6.	Assign the **scheduler-map** to each interface.
	
	• Configure each interface with **scheduler-map** "voip" using the **classifier** defined above.
	
	`interop@M7I# edit class-of-service interfaces fe-1/3/0`
	`interop@M7I# set unit 0 scheduler-map voip`
	`interop@M7I# set unit 0 classifiers dscp avaya-voip`
	`interop@M7I# exit`
	`interop@M7I# edit class-of-service interfaces lsq-1/2/0`
	`interop@M7I# set unit 0 scheduler-map voip`
	`interop@M7I# set unit 0 classifiers dscp avaya-voip`
	`interop@M7I# exit`
	`interop@M7I# edit class-of-service interfaces t1-0/0/0`
	`interop@M7I# set unit 0 scheduler-map voip`
	`interop@M7I# set unit 0 classifiers dscp avaya-voip`
	`interop@M7I# exit`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

7.	Configure the Ethernet and T1 interfaces.
	
	• Configure the Ethernet interface to use the scheduler.
	• Assign an IP address to the interface.
	
	`interop@M7I# edit int fe-1/3/0`
	`interop@M7I# set per-unit-scheduler`
	`interop@M7I# set unit 0 family inet address 172.28.10.254/24`
	`interop@M7I# exit`
	
	• Configure the logical interface for the WAN connection to use the scheduler.
	• Assign an IP address to the interface.
	• Specify the RTP traffic to be compressed. The sample configuration defines RTP traffic with port range 2048 to 3029 to be compressed. This port range needs to match **UDP Port Min** and **UDP Port Max** configured in Avaya Communication Manager in Section 5, Step 8.
	
	`interop@M7I# edit int lsq-1/2/0`
	`interop@M7I# set per-unit-scheduler`
	`interop@M7I# set unit 0 compression rtp port min 2048 max 3029`
	`interop@M7I# set unit 0 family inet 192.168.1.1/30`
	`interop@M7I# exit`
	
	• Configure the T1 interface to use the scheduler.
	• Configure the T1 interface timing, encapsulation, and timeslots.
	• Configure the T1 interface to use logical interface lsq-1/2/0.0 defined above. An IP address is not necessary because an IP address is already defined for the logical interface.
	
	`interop@M7I# edit int t1-0/0/0`
	`interop@M7I# set per-unit-scheduler`
	`interop@M7I# set clocking internal`
	`interop@M7I# set encapsulation ppp`
	`interop@M7I# set t1-options timeslots 1-24`
	`interop@M7I# set unit 0 compression-device lsq-1/2/0.0`
	`interop@M7I# exit`

10.	Configure the routing options for the router. The sample configuration uses static routes.
	
	`interop@M7i# edit routing-options static`
	`interop@M7i# route 172.28.20.0/24 next-hop 192.168.1.2`
	`interop@M7i # exit`

11.	Configure the bootp relay to direct bootp requests to the router. The M7i router was configured to verify the DHCP relay feature during testing. `interop@M7i # set forwarding-options helpers bootp server 192.168.1.2`

©2006 Avaya Inc. All Rights Reserved.

Step	Description
12.	Save the changes. `interop@M7i # commit`

5. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult reference [1], [2], [3], and [4]. The following steps describe the configuration of Avaya Communication Manager at the Main site. Repeat these steps at the Avaya Communication Manager at the Branch site unless otherwise noted.

Step	Description
1.	Add a new station for the Avaya IP Telephones to Avaya Communication Manager using the **add station** command. Make sure the following fields are configured. **Extension:** ***22022*** (Extension number for the Avaya Telephone) **Type:** ***4610*** (Avaya Telephone type used for this extension) **Port:** ***IP*** (Type of connection for the Avaya Telephone) **Security Code:** ***123456*** (Security code used by the Avaya Telephone to register with Avaya Communication Manager) **Direct IP-IP Audio Connections:** ***Y*** (Enable shuffling) The screen below shows station extension 22022. Repeat this step for each station. **add station 22022** **Page 1 of 4** STATION **Extension: 22022** Lock Messages? n BCC: 0 **Type: 4610** **Security Code: 123456** TN: 1 **Port: IP** Coverage Path 1: COR: 1 Name: Room 18 Coverage Path 2: COS: 1 Hunt-to Station: STATION OPTIONS Loss Group: 19 Personalized Ringing Pattern: 1 Message Lamp Ext: 22022 Speakerphone: 2-way Mute Button Enabled? y Display Language: english Survivable GK Node Name: Survivable COR: internal Media Complex Ext: Survivable Trunk Dest? y IP SoftPhone? n Customizable Labels? y

©2006 Avaya Inc. All Rights Reserved.

Step	Description

```
change station 22022                                          Page   2 of   4
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
            CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? y                       Restrict Last Appearance? y
  Active Station Ringing: single          Conf/Trans on Primary Appearance? n
                                                       EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed
        Multimedia Mode: enhanced
    MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name:                     Select Last Used Appearance? n
                                                Coverage After Forwarding? s

                                             Direct IP-IP Audio Connections? y
 Emergency Location Ext: 22022     Always Use? n      IP Audio Hairpinning? y
```

2. Add the S8300 Media Server IP address located at the Branch Site into the Avaya Communication Manager using the **change node-names ip** command. The screen below shows the entry for the Branch Site as **Branch-ACM** with IP address of **172.28.20.5**.

```
change node-names ip                                          Page   1 of   1
                                  IP NODE NAMES
    Name                 IP Address          Name              IP Address
Brach-ACM              172.28 .20 .5                            .   .   .
clan                   172.28 .10 .7                            .   .   .
default                0  .0  .0  .0                           .   .   .
medpro                 172.28 .10 .8                            .   .   .
procr                  172.28 .10 .5                            .   .   .
                          .   .   .                             .   .   .
                          .   .   .                             .   .   .
                          .   .   .                             .   .   .
```


©2006 Avaya Inc. All Rights Reserved.

Step	Description
3.	Configure a signaling group for the H.323 trunk between the Avaya Communication Manager at the Main and Branch Site. Make sure the following fields are configured.

Group Type:	***h.323***	(Signaling type used)
Trunk Group for Channel Selection:		
	1	(This value needs to be completed after Step 4 below has been completed)
Near-end Node Name:	***clan***	(This is the **clan** name defined in Step 2)
Near-end Listen Port:	***1720***	(Default port number for H.323 signaling)
Far-end Node Name:	***Branch-ACM***	(Node name for Branch Site system defined in Step 2)
Far-end Listen Port:	***1720***	(Default port number for H.323 signaling)
Far-end Network Region:	***2***	(Region 1 was used throughout this sample configuration)
Media Encryption	***Y***	(Enable Advanced Encryption Standard [AES] encryption option)

```
display signaling-group 1                                    Page   1 of   5
                               SIGNALING GROUP

 Group Number: 1              Group Type: h.323
                          Remote Office? n          Max number of NCA TSC: 0
                                   SBS? n           Max number of CA TSC: 0
                              IP Video? n        Trunk Group for NCA TSC:
      Trunk Group for Channel Selection: 1
         Supplementary Service Protocol: a          Network Call Transfer? n
                       T303 Timer(sec): 10

   Near-end Node Name: clan                  Far-end Node Name: G350
 Near-end Listen Port: 1720                Far-end Listen Port: 1720
                                         Far-end Network Region: 2
        LRQ Required? n                 Calls Share IP Signaling Connection? n
        RRQ Required? n
    Media Encryption? y                     Bypass If IP Threshold Exceeded? n
          Passphrase: *                             H.235 Annex H Required? n
       DTMF over IP: out-of-band           Direct IP-IP Audio Connections? y
                                                     IP Audio Hairpinning? y
                                              Interworking Message: PROGress
                                        DCP/Analog Bearer Capability: 3.1kHz
```


©2006 Avaya Inc. All Rights Reserved.

Step	Description

4.	Configure an H.323 trunk group. Use the **add trunk-group** command to create a new trunk group.
	
	Group Type: ***isdn***
	TAC: ***101*** (User assigned)
	Carrier Medium: ***H.323*** (Type of trunk)
	Member Assignment Method: ***auto***
	Signaling Group: ***1*** (Signaling group number created in Step 3)
	Number of Members: ***50*** (Number of members for the trunk group used for this sample network)
	
	`add trunk-group 1` `Page 1 of 21`
	`TRUNK GROUP`
	`Group Number: 1` `Group Type: isdn` `CDR Reports: y`
	`Group Name: To G350` `COR: 1` `TN: 1` `TAC: 101`
	`Direction: two-way` `Outgoing Display? n` `Carrier Medium: H.323`
	`Dial Access? n` `Busy Threshold: 255` `Night Service:`
	`Queue Length: 0`
	`Service Type: tie` `Auth Code? n`
	`Member Assignment Method: auto`
	`Signaling Group: 1`
	`Number of Members: 50`

5.	Configure the dial plan to route calls to the Branch Site. Use the **change dialplan analysis** command to configure calls for extension range 3xxxx. The following configures any 5 digit number starting with 3 as an "aar" Call Type. ARS/AAR Dialing without FAC was enabled in the sample configuration. The "display system-parameters customer-options" command can be used to verify if this option is enabled.
	
	`change dialplan analysis` `Page 1 of 12`
	`DIAL PLAN ANALYSIS TABLE`
	`Percent Full: 1`
	
	`Dialed String / Total Length / Call Type` (repeated three times)
	`1 3 dac`
	`2 5 ext`
	`221 5 aar`
	`3 5 aar`
	`4 5 ext`
	`5 5 ext`
	`9 3 fac`

©2006 Avaya Inc. All Rights Reserved.

Step	Description

```
display system-parameters customer-options                    Page   3 of  10
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n           Audible Message Waiting? n
        Access Security Gateway (ASG)? n               Authorization Codes? n
        Analog Trunk Incoming Call ID? n Backup Cluster Automatic Takeover? n
 A/D Grp/Sys List Dialing Start at 01? n                        CAS Branch? n
Answer Supervision by Call Classifier? n                          CAS Main? n
                                  ARS? y                  Change COR by FAC? n
                 ARS/AAR Partitioning? y  Computer Telephony Adjunct Links? n
          ARS/AAR Dialing without FAC? y   Cvg Of Calls Redirected Off-net? n
          ASAI Link Core Capabilities? n                       DCS (Basic)? n
          ASAI Link Plus Capabilities? n                DCS Call Coverage? n
       Async. Transfer Mode (ATM) PNC? n                DCS with Rerouting? n
  Async. Transfer Mode (ATM) Trunking? n
             ATM WAN Spare Processor? n    Digital Loss Plan Modification? n
                                  ATMS? n                          DS1 MSP? n
                   Attendant Vectoring? n             DS1 Echo Cancellation? n
```

6. Configure AAR to use the appropriate route pattern using the **change aar analysis** command. The following shows that when a 5 digit number starting with 3 is dialed, Route Pattern **1** is used.

```
change aar analysis 3                                         Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                                            Percent Full:    1

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    3                    5    5    1         aar          n
    4                    7    7    999       aar          n
    5                    7    7    999       aar          n
```

7. Configure the Route Pattern using the **change route-pattern** command. The following shows calls using route-pattern 1 are routed to trunk group 1 configured in Step 4.

```
change route-pattern 1                                        Page   1 of   3
                   Pattern Number: 1   Pattern Name:
                            SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                            Dgts                                    Intw
 1: 1    0                                                           n   user
 2:                                                                  n   user
 3:                                                                  n   user
```


©2006 Avaya Inc. All Rights Reserved.

Step	Description
8.	Configure the IP network region using the **change ip-network-region** command. Note the values for **UDP Port Min**, **UDP Port Max**, **Call Control PHB Value** and **Audio PHB Value.** These values are needed to configure the cRTP and QoS parameter on the routers. The IP NETWORK REGION form also specifies the codec set that will be used. All intra-region calls are configured to use the default ip-network region of 1 with the same value for parameters mentioned above. Inter-region calls are configured to use ip-network-region of 2 which uses ip-codec-set 2.

```
change ip-network-region 2                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 34      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

```
change ip-network-region 2                                    Page   3 of  19

                   Inter Network Region Connection Management

 src dst  codec  direct                                      Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway    IGAR
 2   1     2       y           :NoLimit                                    n
 2   2     1
 2   3
 2   4
```


©2006 Avaya Inc. All Rights Reserved.

Step	Description
9.	Configure the appropriate audio codec using the **change ip-codec-set** command. The following shows ip-codec-set 2 using G.729B. The G.711MU codec was also verified during the compliance testing. Media encryption was set for both **aes** and **none** to ensure interoperability with AES capable endpoints. **change ip-codec-set 2** **Page 1 of 2** IP Codec Set Codec Set: 2 Audio Codec / Silence Suppression / Frames Per Pkt / Packet Size(ms) **1: G.729B n 2 20** 2: 3: 4: 5: 6: 7: Media Encryption **1: aes** **2: none** 3:
10.	Save the configuration using the **save translation** command. **save translation** SAVE TRANSLATION Command Completion Status — Error Code Success — 0
11.	Repeat Steps 1-10 in this section for Avaya Communication Manager in the Branch Site to complete the configuration. Make sure the appropriate IP address information is entered when configuring the Branch Site. At the Branch site, the "near end" is the Avaya S8300 Media Server and the "far end" is the C-LAN at the Main site.

6. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Juniper Networks routers in supporting an Avaya IP Telephony infrastructure consisting of Avaya Communication Manager and Avaya IP Telephones. A data traffic generator and a call generator were used to simulate background traffic and additional voice flow in a typical network environment.

©2006 Avaya Inc. All Rights Reserved.

6.1. General Test Approach

Quality of Service was verified by injecting simulated data traffic into the network using a traffic generator while calls were being established and maintained using the Avaya IP Telephones. The J4300 router was configured to perform as a DHCP Server to test DHCP option 176 used by the Avaya IP Telephones. DTMF detection was tested using the Intuity AUDIX Voice Mail system configured in the S8300 Media Server.

The objectives were to verify the Juniper M7i and J4300 routers support the following:

- QoS for VoIP traffic
- Compressed RTP over Point-to-Point Protocol
- Point-to-Point Protocol
- DHCP Server support for Option 176
- AES-encrypted VoIP traffic
- Basic calling (e.g. call, transfer, conference, DTMF detection)

6.2. Test Results

The Juniper Networks M7i and J4300 routers successfully achieved all objectives. Quality of Service for VoIP traffic was maintained throughout the testing in the presence of competing simulated traffic. No degradation of Voice quality was detected through the use of compress RTP. The Avaya IP Telephones successfully received appropriate IP addresses from the J4300 router and registered with the correct server. AES-encrypted VoIP traffic was successfully established and maintained through the WAN network.

7. Verification Steps

The following steps may be used to verify the configuration:

- Place inter-site calls between the Avaya IP Telephones.
- Use the “show service crtp flow” command on the Juniper router to verify that RTP traffic is being compressed.
- Use the “show interface queue” command on the Juniper router to verify that VoIP traffic is being prioritized correctly.
- Use the “show class-of-Service forwarding-table” command on the Juniper routers to verify that the appropriate bandwidth is being assigned on the interfaces.

8. Support

For technical support on the Juniper Networks product, contact Juniper Networks JTAC at (888) 314-JTAC, or refer to http://www.juniper.net

9. Conclusion

These Application Notes have described the administration steps required to configure Juniper Networks M7i and J4300 routers to support Avaya Communication Manager and Avaya IP Telephones.

©2006 Avaya Inc. All Rights Reserved.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2.1, May 2006
[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005 Release 3.0
[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 11, February 2006
[4] *Avaya IP Telephony Implementation Guide*, May 1, 2006

Product documentation for Juniper Networks products may be found at http://www.Juniper.net

[5] *CLI User Guide (JUNOS Internet Software for J-series, M-series, and T-series Routing Platform) Release7.6*, Part Number 530-015682-01, Revision 1
[6] *JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Class of Service Configuration Guide Release 7.6*, Part Number 530-015688-01, Revision 1
[7] *JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Network Interfaces Configuration Guide Release 7.6*, Part Number 530-015687-01, Revision 1
[8] *JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Services Interfaces Configuration Guide Release 7.6*, Part Number 530-015687-01, Revision 1

©2006 Avaya Inc. All Rights Reserved.

©2006 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.

©2006 Avaya Inc. All Rights Reserved.